PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 | A1

(11) International Publication Number: WO 00/24154

(43) International Publication Date: 27 April 2000 (27.04.00)

(21) International Application Number: PCT/IL99/00549

(22) International Filing Date: 20 October 1999 (20.10.99)

(30) Priority Data:
09/175,619 20 October 1998 (20.10.98) US

(71) Applicant *(for all designated States except US)*: GALIAD COMPUTERS LTD. [IL/IL]; P.O. Box 23395, 91233 Jerusalem (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: OFIR, Amiram [IL/IL]; 26/5 Shai Street, 91233 Jerusalem (IL).

(74) Agent: FRIEDMAN, Mark, M.; Beit Samueloff, Haomanim Street 7, 67897 Tel Aviv (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

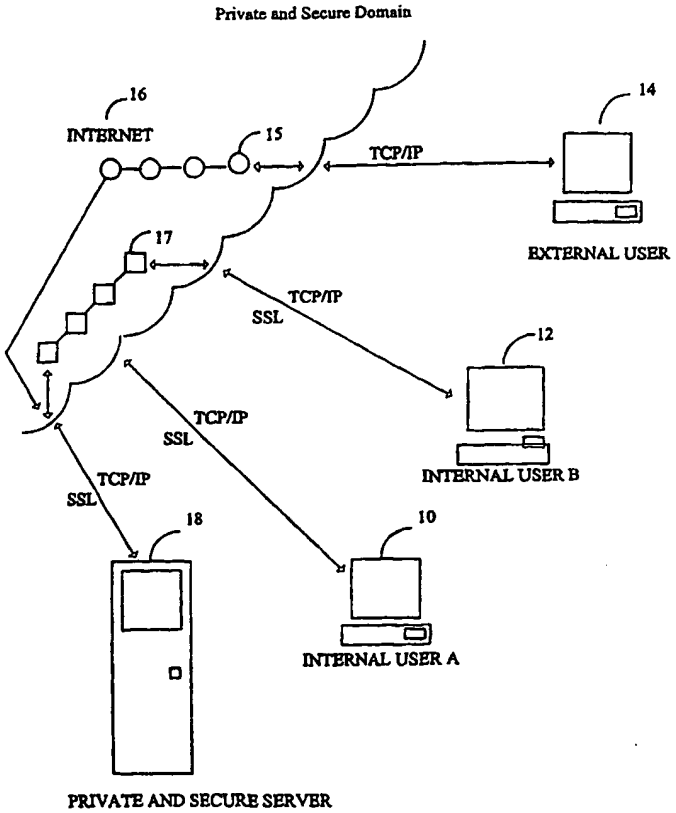
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE MESSAGING SYSTEM AND METHOD

(57) Abstract

A system and a method in which the user (10) can exchange secure data transmissions with other users within (12) or optionally outside (14) of the secured system. The system and method preferably do not require any user intervention for the creation of the secure data, by using transport-layer encryption and authentication technology, including but not limited to the Secure Socket Layer (SSL) encryption and authentication interface (24). In addition, the system and method are suitable for the transmission and display of many different types of messages through a unified user interface. Furthermore, the data contained in these different types of messages may optionally be organized for the user for efficient display and data storage. All of these features are provided through a platform which is widely available and which is simple to operate. Thus, the user preferably does not need to install any additional software programs on the user computer, apart from the web browser software program in order to operate the system and method.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Secure Messaging System and Method

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system and a method for securely sending and receiving messages, and, in particular, a system and method for management of the secure transmission of many different types of messages without active intervention by the user.

E-mail (electronic mail) is used by a large number of people on an international basis, replacing paper office memos, and helping geographically dispersed families and coworkers keep in touch or share information. As the population of computer users come to rely more on e-mail as a mechanism for communication, more e-mail content is requiring privacy. On a private network, the sender connects directly to the server, such that privacy may be more readily assured, by protecting a single peer-to-peer connection. On the Internet, e-mail messages bounce from node to node until they reach their destinations, since connections on the Internet are not peer-to-peer. Unfortunately, such "multihop" connections are easy to intercept, providing many potential opportunities to tamper with an Internet e-mail transmission.

However, when a user browses through the World Wide Web, the computer of the user basically establishes a direct connection to each Web server from which Web page content is requested. Therefore, Web communication can be made secure by securing the channel for data transmission, which is the connection between the user computer and the Web server. Since Internet e-mail can pass through several servers before reaching the final destination, securing such a communication channel is impossible. Instead, the e-mail message itself must be secured.

Providing secure transactions across the Internet has three goals. First, two parties engaging in a transaction, such as the exchange of e-mail, a business transaction, or some other data transfer, do not want a third party to be able to read the transmission. Therefore, data encryption is required in order to satisfy this goal. Second, the recipient of the message should be able to detect whether tampering with the e-mail message has occurred in transit, which requires a message integrity scheme. Finally, both parties must know that they are communicating with the actual person and not with an impostor. This is done with user authentication.

There are several proprietary mechanisms to encrypt and secure electronic communications, although none of these proprietary mechanisms fully satisfies these three goals for e-mail messages. Traditional, single-key encryption, in which the same key is used to both

encrypt and decrypt messages, is unworkable for e-mail communications because there is no safe way to transmit the key. On the one hand, sending the key unencrypted is not safe. On the other hand, delivering the keys manually to e-mail recipients, who may be at a geographically distant location, is highly inconvenient. Thus, single-key encryption is not useful for e-mail messages.

As is known in the background art, one way to transmit a key safely is to use a technique called dual-key or asymmetric encryption, which has separate keys for encrypting and decrypting. Public keys are used to encrypt the messages sent to recipients, while the recipients use their private keys to decrypt these messages. The two keys are mathematically related, but the private key cannot be derived from the public key, so the public key can be freely distributed. The private key does not need to be transmitted beyond the computer of the private key owner.

An example of the operation of such a dual-key system is as follows. When User A wants to send a secure message to User B, User A encrypts the message with User B's public key. When User B receives the message, User B decrypts the message with User B's private key. However, using this method requires User A, the sender, to first obtain the public key of User B, the recipient. Two popular public-key software packages which use the dual-key encryption method are PGP (Pretty Good Privacy) and S/MIME (a secure version of the popular data compression utility MIME).

Unfortunately, there are several problems with the dual-key solution for encryption. One problem arises when a user wants to send encrypted e-mail to recipients who are not known to the user. In this case, the sender does not know which public key belongs to the recipient. Another problem with client-side dual-key encryption is that the encryption process is computationally intensive and requires a significant amount of time to perform.

A more useful solution would provide a secure mechanism for sending many different types of messages, including e-mail messages, without requiring user intervention. Such a solution would be transparent and effective over a widely available platform. Furthermore, such a solution would also provide organization for these different types of messages, in order to display and store the information contained in these messages to the user in the most efficient manner. Unfortunately, such a solution is not currently available.

There is therefore a need for a system and a method which provides a solution for all three issues of secure data transmission, including but not limited to, encryption, tampering and authentication over the Internet, which is efficient, which requires minimal user intervention and which also is useful for managing many different types of messages.

SUMMARY OF THE INVENTION

The present invention is of a system and a method in which the user can exchange secure data transmissions with other user(s) within or optionally outside of the secured system. The system and method preferably do not require any user intervention for the creation of the secure data, by using transport-layer encryption and authentication technology, including but not limited to, the Secure Socket Layer (SSL) encryption and authentication interface. In addition, the system and method are suitable for the transmission and display of many different types of messages through a unified user interface. Furthermore, the data contained in these different types of messages may optionally and preferably be organized for the user for efficient display and data storage. All of these features are provided through a platform which is widely available and which is simple to operate, which is preferably the GUI (graphical user interface) display provided by Web browser software programs. Thus, the user preferably does not need to install any additional software programs on the user computer, apart from the Web browser software program, in order to operate the present invention.

According to the teachings of the present invention there is provided a system for providing a private and secure message through a standard GUI (graphical user interface) platform, the system comprising: (a) a sender computer for sending a message through the GUI platform; (b) a central, secure server for receiving the message from the sender computer; (c) a recipient computer for viewing the message from the central secure server through the GUI platform; and (d) a secure channel for automatically securing and authenticating the message between the central secure server and at least one of the sender computer and the recipient computer.

According to another embodiment of the present invention, there is provided a method for securing a data transmission between a sender for sending and a recipient for receiving the data transmission, the method comprising the steps of: (a) providing a server; (b) providing a secure channel connected to the server; (c) sending a data transmission from the sender to the server through the secure channel such that the data transmission is substantially automatically secured and authenticated; (d) sending the data transmission from the server to the recipient; and (e) receiving the data transmission by the recipient.

Hereinafter, the term "Web browser" refers to any software program which can display text, graphics, or both, from Web pages on World Wide Web sites. Hereinafter, the term "Web page"

refers to any document written in a mark-up language including, but not limited to, HTML (hypertext mark-up language) or VRML (virtual reality modeling language), dynamic HTML, XML (extended mark-up language) or related computer languages thereof, as well as to any collection of such documents reachable through one specific Internet address or at one specific World Wide Web site, or any document obtainable through a particular URL (Uniform Resource Locator). Hereinafter, the term "Web site" refers to at least one Web page, and preferably a plurality of Web pages, virtually connected to form a coherent group. Hereinafter, the term "Web server" refers to a computer or other electronic device which is capable of serving at least one Web page to a Web browser.

Hereinafter, the term "network" refers to a connection between any two or more computers which permits the transmission of data, including but not limited to, the Internet.

Hereinafter, the phrase "display a Web page" includes all actions necessary to render at least a portion of the information on the Web page available to the computer user. As such, the phrase includes, but is not limited to, the static visual display of static graphical information, the audible production of audio information, the animated visual display of animation and the visual display of video stream data.

Hereinafter, the terms "computer user" and "user" both refer to the person who operates the Web browser or other GUI interface and navigates through the system of the present invention by operating a computer.

Hereinafter, the term "computer" refers to a combination of a particular computer hardware system and a particular software operating system. Examples of such hardware systems include those with any type of suitable data processor. Hereinafter, the term "computer" includes, but is not limited to, personal computers (PC) having an operating system such as DOS, Windows™, OS/2™ or Linux; Macintosh™ computers; computers having JAVA™-OS as the operating system; and graphical workstations such as the computers of Sun Microsystems™ and Silicon Graphics™, and other computers having some version of the UNIX operating system such as AIX™ or SOLARIS™ of Sun Microsystems™; a PalmPilot™, a PilotPC™, or any other handheld device; or any other known and available operating system. Hereinafter, the term "Windows™" includes but is not limited to Windows95™, Windows 3.x™ in which "x" is an integer such as "1", Windows NT™, Windows98™, Windows CE™ and any upgraded versions of these operating systems by Microsoft Corp. (USA).

For the present invention, a software application could be written in substantially any suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer by which the software application is executed, and in particularly with the operating system of that computer. Examples of suitable programming languages include, but are not limited to, C, C++ and Java. Furthermore, the functions of the present invention, when described as a series of steps for a method, could be implemented as a series of software instructions for being operated by a data processor, such that the present invention could be implemented as software, firmware or hardware, or a combination thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

FIG. 1 is a schematic block diagram of an exemplary system according to the present invention;

FIG. 2 is a schematic block diagram of the standard, background art OSI Interface, with the Secure Socket Layer diagrammed;

FIG. 3 a schematic block diagram of the standard, background art Secure Socket Layer 3.0;

FIG. 4 is a flowchart of an exemplary method for sending a message from an internal user to another user according to the present invention;

FIG. 5 is a flowchart of an exemplary method for sending a message from an external user to an internal user according to the present invention;

FIG. 6 is a flowchart of an exemplary method for managing information related to an "address" or contact book according to the present invention;

FIG. 7 is a flowchart of an exemplary method for managing information related to messages posted to a bulletin board according to the present invention; and

FIG. 8 is a flowchart of an exemplary method for managing scheduling information according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is of a system and a method, in which the user can exchange secure data transmissions with other user(s) within or optionally outside of the secured system. The system and method preferably do not require any user intervention for the creation of the secure data, by using transport-layer encryption and authentication technology, including but not limited to, the Secure Socket Layer (SSL) encryption and authentication interface. More preferably, the SSL encryption and authentication interface is used for securing the messages, since SSL is an industry standard for Web browser software programs and is provided as an automatic feature of these programs, such that the user could preferably operate the system of the present invention through the standard Web browser software program interface. Thus, the user preferably does not need to install any additional software programs on the user computer, apart from the Web browser software program, in order to operate the present invention.

In addition, the system and method of the present invention are suitable for the transmission and display of many different types of messages through a unified user interface. Furthermore, the data contained in these different types of messages may optionally and preferably be organized for the user for efficient display and data storage. All of these features are provided through a platform which is widely available and which is simple to operate, which is preferably the GUI (graphical user interface) display provided by Web browser software programs. As previously described, more preferably the user does not need to install any additional software programs or "plug-ins" to the Web browser software program, such that the present invention is operable with the standard Web browser software program alone. Therefore, the Web browser interface preferably provides the single, unifying interface for viewing the data contained in the messages, and for operating the system of the present invention to send and receive such messages.

Therefore, the system and the method of the present invention have a number of advantages over the background art. First, the present invention does not require the provision or exchange of public and/or private data encryption keys by the sending and receiving users. Second, the present invention does not require special, proprietary software, but preferably operates only with a Web browser which complies with the industry standard for SSL. Third, the present invention organizes and manages data from many different types of messages, which is not provided in the background art.

The principles and operation of the system and method according to the present invention may be better understood with reference to the drawings and the accompanying description. Although the description of Figures 1-5 focuses upon the transmission of e-mail messages, it is understood that this is for the purposes of illustration only and is without any intention of being limiting, as the system and method of the present invention are useful for the secure transmission of many different types of messages. Figures 6-8 describe additional examples of messages for which the system and method of the present invention are also useful, including information related to an "address" or contact book (Figure 6), messages posted to a bulletin board or "chat room" (Figure 7) and the arrangement of scheduling information (Figure 8).

Referring now to the drawings, Figure 1 is a schematic block diagram of an exemplary private and secure system according to the present invention, with a server **18** containing the mailboxes for internal users **10,12** and external users **14** using standard Web browser software programs to communicate over the Internet **16**. As will be appreciated by those skilled in the art, standard access to e-mail is accomplished via a modem connection to an Internet Service Provider who provides a temporary Internet address for the user connection and typically a mailbox for that user to receive and send mail. Connections to the Internet use the standard TCP/IP protocol which is further explained in Figure 2. All e-mail transmissions sent and received are unencrypted unless the sender and recipient have exchanged public keys beforehand and are using software like PGP or S/MIME to encrypt/decrypt the message.

In the system of Figure 1, Internal User A **10** connects to Private and Secure server **18** through a login interface which requires a proper username and password combination. By "internal", it is meant that User A **10** is a member of the system of secure e-mail transmission which is provided by Private and Secure server **18**, such that Internal User A **10** may both send and receive secure e-mail through Private and Secure server **18**. Internal User A **10** then gains access to the encrypted e-mail inbox, containing encrypted data. Encrypted data **17** is sent to the browser of Internal User A **10** through a secure channel, such as the Secure Socket Layer channel, on Private and Secure server **18** and unencrypted automatically by the Secure Socket Layer implementation built into the Web browser of Internal User A **10**.

External users **14** could also connect to the Private and Secure server **18** via standard e-mail software and send unencrypted data **15** to an Internal User **10** or **12** on Private and Secure server **18**. By "external", it is meant that External User **14** cannot send secure e-mail messages through Private and Secure server **18**, although optionally and preferably, External User **14** can

receive e-mail messages from Private and Secure server 18. As described in greater below with regard to Figure 4, these e-mail messages are not sent securely to External User 14, unless External User 14 is given a temporary and/or limited function account with Private and Secure server 18, in which case External User 14 would receive messages in a similar manner as Internal User 10 or 12, for example.

Secure Socket Layer channel encryption occurs away from the user-interface, as illustrated in Figure 2, which shows the diagram of the Open System Interconnection (OSI) Interface for standard network architecture, which was developed by the International Standards Organization.

The OSI model is composed of seven different layers. Each layer has its own function, adding information to the message to ensure it reaches the correct destination without errors. Information added to the beginning of a message is called a header. Information added to the end of the message is called a trailer. A message travels through the OSI layer in segments. The layers append an information-bearing header to each segment and a trailer to the end of the message. At the receiving end, corresponding or peer layers interpret information and implement commands in the header and trailer. Then they remove the header and trailer and transmit the data as intended by the sender.

Protocols are rules agreed upon by the sender and receiver which specify data communications techniques and procedures. TCP/IP (Transmission Control/Internet Protocol) is an implementation of two layers of the OSI model. TCP, the transmission control protocol, divides transmissions into packets, reassembles them at the receiving end in the correct order, and resends portions that do not transmit correctly. IP, the Internet protocol, is responsible for the actual routing and transmission of data.

While each of the seven layers in the OSI model contribute their share in the successful transmission of data, with regard to the present invention there are two layers that are of particular significance, the Application layer, block 21 and the Transport layer, block 25. Secure Socket Layer (SSL) software resides at the TRANSPORT layer, block 25, (also known as the "connection" layer) which is where TCP/IP also partially resides. This layer is several layers away from the user and APPLICATION layer, block 21, where HTTP, FTP and TELNET reside, illustrating that the actions of SSL occur away from the user interface.

As previously mentioned, one of the problems with the background art PGP or S/MIME implementations of dual-key encryption is the necessity for the sending user to somehow verify

the public-key with the recipient. An automated solution is provided by Secure Socket Layer (SSL); however, this invention is not limited to the solution provided by SSL. SSL is brought here only as an example of a solution which requires no user intervention in the encryption, message integrity and authentication aspects of a secure data transfer. Using SSL, a client program and a server program agree on encryption, MAC (Message Authentication Code) methods and key-exchange methods. Key-exchange methods can include but are not limited to, DH (Diffie-Hellman) and DHE, which are non-proprietary methods developed by Whitfield Diffie and Martin Hellman; or an RSA method developed by RSA Data Security. SSL 3.0 requires that the client and server agree on a set of randomly generated keys.

SSL 3.0 provides a solution for user-authentication by using Digital Certificates. Digital Certificate standards include DSS, the Digital Signature Standard approved by the National Institute of Standards and Technology in 1994, or a proprietary certificate signed using RSA Data Security technology. A Certificate Authority is a bureau offering Authentication Signature to sites who would wish to offer SSL service to Internet Browsers. A site which wants to offer SSL needs to send authenticating information to a Certificate Authority. The reply from the Certificate Authority is the authenticating information, "Signed" by the private key and public key of the Authority, which forms a "Site Certificate". The signature can be authenticated by any individual with the public key of the Authority.

According to SSL, a Web Browser always uses encryption to exchange information with a secure site. For every session, the Web Browser generates a new encryption key and sends the key to the Web Server before communication starts. Both Web Browser and Web Server use this key to encrypt any information they exchange. The following steps are taken by the Browser to initiate a connection with a secure site. First the Browser requests the Site's Certificate, which contains the Site's information including name, name of Certificate Authority, Public Key, "Finger Prints" and "Signature". Then the Browser authenticates the site using the Certificate Authority's public key. Next, the Browser produces an encryption key, and encrypts this key with the server's public key. The encrypted key is then sent to the Web Server. Finally, communication of the data can begin.

Figure 3 is a flow diagram that illustrates how Secure Socket Layer 3.0 implements the sending of a secure document (more detailed information can be found in the book "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption" by Warwick Ford and Michael S. Baum, ISBN# 0134763424, incorporated as if fully set forth

herein only for the purpose of describing SSL). The sender sends a document to the recipient, block 30. The message-digest function (MD5 or SHA) then produces a MAC (Message Authentication Code), block 31. The MAC is encrypted with the sender's private key, block 32. The encryption methods can optionally include non-proprietary encryption methods specified by the Data Encryption Standard approved by the National Institute of Standards and Technology in 1994 such as DES, DES40, 3DES, or proprietary encryption methods developed by RSA Data Security such as RC2_CBC_40, RC4_128 and RC_40. In block 33 the encrypted MAC is attached to the document, and both the encrypted MAC and the document are encrypted with the recipient's public key.

The message is sent to the recipient via standard Internet communication, block 34. In block 35 the recipient receives the message and decrypts it with the recipient's private key. The recipient produces a local copy of the document's MAC by using the same message-digest function that the sender used, block 37. The recipient compares the local copy of the MAC, block 38 to the unencrypted MAC, block 39. If they are identical, then the document has not been tampered with and only the sender could have created the original message.

Turning now to the system and method of the present invention, Figure 4 is a flow diagram of how an Internal User sends data transmissions to other users external to the Private and Secure System according to the present invention. Optionally and preferably, four choices are offered to the Internal User with regard to the transmission of e-mail messages, or other messages, to users who are external to the secure system. More preferably, these choices are configured by the user and/or by a system manager as part of the "preferences" for operating the secure system according to the present invention.

The first choice is for the system to refuse to send such a message, such that the user would receive a system notification, indicating that the message could not be sent since the intended recipient is external to the secure system. This choice may be preferred since messages cannot be sent securely to external recipients. The message would be sent securely from the user computer to the central secure server. However, the message would need to be sent as plaintext, without encryption or other secure protection, from the central secure server to the computer of the intended recipient who is external to the secure system. Thus, a more secure policy would optionally prevent such messages from being sent.

The second choice would simply notify the Internal User if such a non-secure message is to be sent to the external user. For example, the Internal User would optionally need to indicate

acceptance of the transmission of the e-mail message to an external, non-secure user, by "clicking" on a GUI gadget, or otherwise indicating acceptance of such a non-secure transmission. The Internal User would thus be given the choice each time as to whether the non-secure e-mail message is to be sent to a user who is external to the secure system of the present invention.

The third choice, described in greater detail below, would provide a temporary, limited account for the external user to be able to read the message from the secure central server. The external user could then receive a secure message within the secure system of the present invention.

The fourth choice is simply to allow all such non-secure messages to be sent, without notifying or alerting the Internal User. Of course, such a choice has the disadvantage that the e-mail message, or other message, would be sent without secure protection, as well as the further disadvantage that the Internal User would not necessarily be aware that the message is being sent to a user who is external to the secure system of the present invention.

The specific preferred implementation of these choices is as follows. In the embodiment of Figure 4, the user establishes a routine connection to the Internet using an SSL (or similar technology) enabled browser. The sender, for example Internal User A **10** of Figure 1, then connects to the Private and Secure server **18** and "log in" or gains access by using a valid name and password combination, block **50**. In decision block **51** the username/password combination is verified. Then sender Internal User A **10** composes the message(s) and attaches any file(s) or other data and sends the e-mail message to another user, block **52**. A unique reference number is generated for that transmission, block **53**. The e-mail message is encrypted and authentication information is attached, unless suppressed by the sender user, block **54**. This process optionally and preferably occurs automatically, for example by implementing SSL or a similar technology.

In decision block **55**, the system determines whether the user is internal or external to the system. In one embodiment, where the recipient is an internal user such as Internal User B **12**, the message is then stored in the inbox of Internal User B **12** on Private and Secure server **18**, as shown in block **60**. In block **61**, Internal User B **12** reads or rejects the e-mail message. A confirmation message is then sent to the sender, who is Internal User A **10**, as shown in block **62**.

In another embodiment, if in block **55** it is determined that the recipient is an external user to the system such as External User **14**, a decision is then taken in block **56** to determine if

data is allowed to be exchanged with external users. In one preferred embodiment such as an intranet (a network of computers which is private to a specific group or organization such as a company), where external data transmissions are not permitted, this transmission would optionally be rejected.

In a further embodiment, where exchanges of data with external users are permitted, a new user is created with a random password, block 57. The e-mail is then stored in the new user's inbox, block 58. In block 59, an e-mail message is generated automatically and sent to External User 14 containing a time-stamped message indicating that there is at least one e-mail message waiting in the inbox on Private and Secure Server 18, which can be accessed with the name and password contained in the e-mail message. The External user 14 then logs on to the Private and Secure server 18 and reads or rejects the e-mail message sent, block 61. A confirmation message is then sent to the sender Internal User A 10, block 62.

Figure 5 is a flow diagram of the process according to the present invention which occurs when an external user to the Private and Secure server 18 attempts to send an e-mail message to an internal user. In this embodiment, assume External User 14 sends an e-mail message via conventional e-mail software to Internal User A 10, a recipient on the Private and Secure Server 18, block 70. The software on the Private and Secure server 18 determines if the recipient is a valid user on the system, decision block 71. In block 72 a unique reference number is generated for the e-mail message. The e-mail message is then time-stamped and stored in the inbox of the recipient Internal User A 10 unencrypted, block 73. In block 74 a time-stamped e-mail message generated by the system is sent back to External User 14, stating that the message was accepted at Private and Secure system 18 for Internal User A 10. The message includes the time when Internal User A 10 last interacted with the system. Optionally and preferably, a warning statement that the message traveled through the standard unprotected e-mail system is included as well. Once Internal User A 10 reads or rejects the mail, block 75, a confirmation message is then sent to the sender External User 14, block 76.

According to preferred embodiments of the present invention, a number of additional features of the present invention optionally and preferably may be included. For example, preferably according to the present invention, all user details for interacting with the system of the present invention are stored on the secure server, such that these details are available to the user regardless of which computer the user uses. Furthermore, all of the messages and related information are also preferably stored on the secure server, in order to both maintain the security

of this data, and to enable the user to access the data from substantially any computer which has a connection to the secure server, for example through the Internet, and which operates a standard Web browser or other standard GUI platform.

In the previously described preferred embodiment of the present invention, these features are enabled by the SSL encryption and secure transmission protocol which is provided through currently available, standard Web browser software programs. The SSL protocol ensures that all data, regardless of content, is encrypted and thereby secured, in a manner which is transparent to the user. The optional but preferred extensions to the present invention, which are described below in greater detail, are operable with the SSL protocol in a substantially similar manner to the transmission of e-mail messages which was previously described.

An example of an additional, preferred feature of the system and method of the present invention is the provision of an "address" or contact book, as described with regard to Figure 6 below. The address book preferably includes multiple records. Information that may be optionally added to the address book may include e-mail address, group or groups to which the user belongs, address and other personal information, for example, company information, telephone numbers, and comments. This information may be optionally available to other users by setting optional flags. Users may also optionally select from whom they should accept messages, for example internal and/or external users.

According to other preferred embodiments, the system of the present invention is a messaging system which is provided through the Web browser interface by using personal addresses and other information which is stored on a central Web server, and as such can be used from anywhere, on any computer without prior setup. This approach means that personal e-mail parameters such as address books are optionally available to the user on the private and secure server and not on the actual machine being used to communicate with the private and secure server.

Figure 6 is a flowchart of a method according to the present invention for managing such an address book, which is stored on the central secure server and is displayed by the Web browser or other standard GUI. The management of the address book includes several features, such as the addition of information concerning a new contact; the option of sharing at least some information with another user in a "read only" manner; and the option of allowing at least one other user to edit at least some of the information in the address book.

As shown in step 1, information is entered into the address book concerning a new contact, such as the name of an individual, e-mail address, telephone number and so forth. Although as for other electronically stored address books, the user may enter such information, according to a preferred embodiment of the present invention, the user receives a request to add the information automatically from another user, who may be either the new contact or a third party. In step 2, the user then has the option to allow or disallow this request.

In step 3, the user optionally sets a flag to allow at least one other user to read at least a portion of the information in the address book. The user may be identified as an individual, or as a member of a group, such as "fellow employee", for example. The information may be segregated according to type of contact, such that some contacts are labeled "private", while others are "public"; according to the type of information, such that the name and e-mail address of contacts are public, but not the telephone number; or a combination thereof, for example.

In step 4, the user optionally and preferably allows at least one other user to edit at least a portion of the information stored in the address book. For example, a secretary may be allowed to enter information concerning a new contact into the address book of a manager, and/or to edit existing information, for example to change information concerning a known contact to update the contact information. Thus, the address book according to the present invention optionally allows the user to share information, and even to permit one or more other users to edit the stored information.

Figure 7 is a flowchart of an exemplary method for managing information related to messages posted to a bulletin board according to the present invention. In step 1, the bulletin board is provided for displaying messages, and is stored on the central secure server of the present invention. In step 2, a set of permissions is determined for the bulletin board, optionally for each message on the board, and alternatively or additionally for each user who has access to the bulletin board. For example, only one or more specific users may be allowed to write new messages to the board, and/or to edit the board. Other users may be given permission to read certain messages, or even all messages on the board.

In step 3, access to the bulletin board is provided from the standard GUI platform, preferably a Web browser, to the secure central server through a secure channel, such as through SSL for example. Therefore, each message is transmitted and read securely, from substantially any computer which both operates the Web browser and is connected to the secure central server.

In step 4, a user reads or otherwise interacts with at least one message of the bulletin board, through the Web browser and secure communication channel.

A variation of the bulletin board is the "chat" function according to the present invention, in which messages are exchanged between at least two parties. If messages are exchanged between more than two parties, then the chat function may be referred to as a "chat room". According to the present invention, each participant in the chat reads the text messages from the central server, preferably without downloading in order to maintain security. Therefore, although the user may optionally be notified of the existence of such a chat message, for example through the POP (Point of Presence) protocol, the user preferably must still read the message through the Web browser connected to the secure central server. Thus, unlike background art chat systems such as ICQ™ (Mirabilis Inc., Israel), the chat function of the present invention is not peer-to-peer, but rather is client-server, with the user operating a Web browser (the client) for receiving information from the secure central server of the present invention.

For a "chat room", the process of enabling users to receive the chat-related messages may optionally and preferably be controlled by a controlling user, who authenticates each user who wishes to join the chat room. Again, the process is a "client-server" process, in which each user must actively read the chat messages which are held on the central server. The process of "chatting" is therefore asynchronous, in that a user posts a message and then waits for the intended recipient(s) to read the message. However, preferably other users are notified when a user leaves the "chat", or stops reading these messages.

Optionally and preferably, the user may receive a transcript of the chat session messages in which the user participated upon leaving the chat session. Also optionally and preferably, these chat functions may be implemented for different types of message data, including but not limited to, voice data, text data and a combination thereof. If audio data such as voice data is to be included, then the hardware components of the user computer would preferably also include a microphone and sound card for receiving and playing the audio data, respectively. More preferably, the management and playing of such audio data would be performed by a software program intended for such purposes, which would preferably interact with the present invention through the unifying user interface of the system of the present invention.

Figure 8 is a flowchart of an exemplary method for managing scheduling information according to the present invention. The scheduling information optionally and preferably includes such information as the date and time of a meeting or other appointment; the expected

duration of the appointment; the location of the appointment, such as at the office of the user or outside of the office of the user; and so forth. Furthermore, preferably all of the requests are sent as messages through the secure system of the present invention, while the scheduler itself is stored on, and operated by, the secure server of the present invention. Thus, this system is preferably implemented in a similar manner as for the previously described address book according to the present invention.

In step 1, a first user sends a request for a meeting to a second user. The request includes such particulars as the date, time, location and optionally the subject of the meeting. In step 2, the scheduler of the first user optionally and preferably shows a tentative appointment time marked for the meeting.

In step 3, the second user receives the appointment request. In step 4, if the second user accepts the request, then the appointment is preferably automatically marked in the scheduler of the second user, optionally with the associated information as previously described. In step 5, once the second user has accepted the request, an acceptance reply is preferably automatically sent to the scheduler of the first user. In step 6, preferably the scheduler of the first user then automatically changes the "tentative" designation of the meeting to "actual" or some other designation indicating that the request has been accepted.

As previously mentioned, optionally and preferably according to the present invention, a user may authenticate another user. This mechanism enables full authentication within the system. For example, any user may ask and receive as many authentications as required. Authentication information is preferably automatically attached to all e-mail transmissions sent from that user. The user may optionally suppress this feature and require no authentication.

Using the optional features thus far described, the user may optionally create private sub-groups. These sub-groups may optionally be "open" or "closed". An open sub-group may consist of users who are authenticated by the same user. A message received by one member from another member can be trusted and if desired, the receiver can identify who the sender was. Additionally users in this group may optionally receive messages from users outside the group. In a closed sub-group, all users who are authenticated by the same user may optionally restrict access to their information section and may optionally not accept messages from any user not in the group. Optionally and preferably, every message composed and sent by both internal and

external users will generate a unique reference number, which is visible to both the sender and recipient.

The present invention has a number of advantages over the prior art, particularly in the preferred implementation of Web browser-based messaging. The Web browser-based messaging system provides a total solution to the transmission of e-mail messages and other types of messages including attachments, without the need for any of the hardware or software required by other systems. The following is a partial list of items required by other messaging systems, which are preferably not required and/or used by the Private and Secure messaging system of the present invention: Firewall, Intranet, Router blocking, Plug-Ins, Helpers and Cookies. Any end-user wishing to use the Private and Secure messaging services of the present invention preferably needs only a computer, access to the Internet and a Web Browser or other widely available, non-proprietary GUI which supports SSL or whatever secure channel technology is used. The user can access data transmissions exchanged with recipients safely, easily and in complete privacy. There is total security from the moment a transmission is sent from the sender to the moment it is received by the recipient. All files that are waiting on the server or stored there are protected by encryption.

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the spirit and the scope of the present invention.

WHAT IS CLAIMED IS:

1. A system for providing a private and secure message through a standard GUI (graphical user interface) platform, the system comprising:

(a) a sender computer for sending a message through the GUI platform;

a central, secure server for receiving said message from said sender computer;

(c) a recipient computer for viewing said message from said central secure server through the GUI platform; and

(d) a secure channel for automatically securing and authenticating said message between said central secure server and at least one of said sender computer and said recipient computer.

2. The system of claim 1, wherein the standard GUI platform is a Web browser software program and said central secure server is a Web server.

3. The system of claim 2, wherein said secure channel is implemented according to the SSL (Secure Socket Layer) protocol.

4. The system of claim 2, wherein said message is an e-mail (electronic mail) message.

5. The system of claim 2, wherein said message is a bulletin board message for storage on a bulletin board, said bulletin board being stored on said Web server, and said bulletin board message being displayed by said Web browser.

6. The system of claim 2, wherein said message includes contact information for an address book, said address book being stored on said Web server, and said contact information being displayed by said Web browser.

7. The system of claim 2, wherein said message is a scheduling message for scheduling an appointment in a scheduler, said scheduler being stored on said Web server, said scheduling message being displayed by said Web browser, said recipient computer sending an automatic acceptance message to said sender computer through said Web server.

8. The system of claim 2, wherein said message is a chat message, said chat message being stored on said Web server and displayed by said Web browser.

9. The system of claim 1, further comprising:

(e) a confirmation message being sent to said sender after said message is sent over said secure channel.

10. The system of claim 1, wherein said server stores said message and said message is encrypted through said secure channel.

11. The system of claim 1, wherein said sender computer connects to said server through said secure channel to send said message to said recipient.

12. The system of claim 11, wherein said recipient computer receives said data transmission by connecting to said server through said secure channel.

13. The system of claim 11, wherein said recipient computer is external to said secure channel and said recipient computer receives notification from said server to facilitate access to said message from said server.

14. The system of claim 13, wherein said notification enables said recipient to connect to said server within said secure channel.

15. The system of claim 1, wherein said secure channel is constructed according to Secure Socket Layer protocol (SSL).

16. The system of claim 15, wherein said secure channel secures connection by encrypting all communication from and to said secure channel.

17. The system of claim 16, wherein a Certificate Authority is used to provide an authentication signature and public key used to encrypt data over said secure channel.

18. The system of claim 1, wherein said sender computer is external to said server and sends said message to said server, and said recipient computer receives said data transmission by connecting to said server.

19. The system of claim 1, wherein said server is a domain containing at least one said server, such that servers in said domain are connected through a plurality of secure channels.

20. A method for securing a message for transmission from a sender computer to a recipient computer, the method comprising the steps of:

(a) providing a secure central server;

(b) providing a secure channel connected from at least the sender computer to said secure central server;

(c) sending the message from the sender computer to said secure central server through said secure channel such that the message is automatically secured and authenticated;

(d) sending the message from said secure central server to the

recipient computer; and

(e) receiving the message by the recipient computer.

21. The method in claim 20, the method further comprising the steps of:

(f) generating a unique reference number for identifying each message; and

(g) sending a confirmation message from said secure central server to the sender computer after the recipient computer reads the message, identified according to said unique reference number.

22. The method in claim 20, wherein step (d) further comprises the steps of:

(i) determining if the message is to be sent to a recipient computer connected to said secure central server through a non-secure channel; and

(ii) sending the message to the recipient computer only if the recipient computer is connected to said secure central server through said secure channel.

23. The method in claim 20, wherein step (d) further comprises the steps of:

(i) determining if the recipient computer is connected to said secure central server through a non-secure channel;

(ii) if the recipient computer is not connected to said secure central server through said secure channel, sending a notification to the recipient computer that the message is waiting on said secure central server;

wherein step (e) includes the step of connecting the recipient computer to said secure central server through said secure channel.

24. The method in claim 20, further comprising the steps of:

(f) logging on to said server from a computer through an Internet connection with a Web browser capable of supporting said secure channel.

25. The method in claim 20, further comprising the steps of:

(f) receiving a site signature from a Certificate Authority for said secure central server;

(g) authenticating the sender computer by sending said transmission through said secure channel with said site signature.

26. The method in claim 20, further comprising the steps of:

(f) creating sub-groups of users; and

(g) determining if a data transmission is accepted according to said sub-groups.

27. The method of claim 20, wherein the sender computer includes a standard GUI platform for sending the message, and the recipient computer includes said standard GUI platform for displaying the message.

28. The method of claim 27, wherein said standard GUI platform is a Web browser software program and said central secure server is a Web server.

29. The method of claim 28, wherein said secure channel is implemented according to the SSL (Secure Socket Layer) protocol.

30. The method of claim 28, wherein the message is an e-mail (electronic mail) message.

31. The method of claim 28, wherein the message is a bulletin board message, wherein step (c) includes the step of storing the message on a bulletin board, said bulletin board being stored on said Web server, and wherein step (e) includes the step of displaying said bulletin board message by said Web browser of the recipient computer.

32. The method of claim 31, wherein said bulletin board is accessible to a plurality of users, the method further comprising the step of:

(f) determining a permission for at least one user for accessing at least one message on said bulletin board; and

(g) permitting access to said at least one user for viewing said at least one message according to said permission.

33. The method of claim 28, wherein the message includes contact information for an address book, wherein step (c) includes the step of adding said contact information to said address book, said address book being stored on said Web server, and wherein step (e) includes the step of displaying said contact information by said Web browser.

34. The method of claim 33, wherein at least a portion of said address book is accessible to a plurality of users, said address book being controlled by a primary user, the method further comprising the steps of:

(f) adding contact information to said address book by one of said plurality of users other than said primary user through said secure channel, such that said one of said plurality of users operates a computer connected to said secure central server through said secure channel.

35. The method of claim 28, wherein the message is a scheduling message for scheduling an appointment in a scheduler, wherein step (c) includes the step of adding said appointment to said scheduler, said scheduler being stored on said Web server, said scheduling message being displayed by said Web browser of the recipient computer, the method further comprising the step of:

(f) if said appointment is accepted, sending an automatic acceptance message from the recipient computer to the sender computer through said Web server.

36. A method for instant messaging through a client/server system, the method comprising the steps of:

(a) providing a secure channel for connecting each client to the server;

(b) sending a message from a first client to the server;

(c) holding said message on the server; and

(d) displaying said message by a second client from the server.

37. The method of claim 36, wherein each client is a Web browser, the server is a Web server, and said secure channel is a SSL (secure socket layer) protocol channel.

38. The method of claim 37, wherein step (c) further comprises the step of notifying said second client of said message being held on the server.

Figure 1 Private and Secure Domain

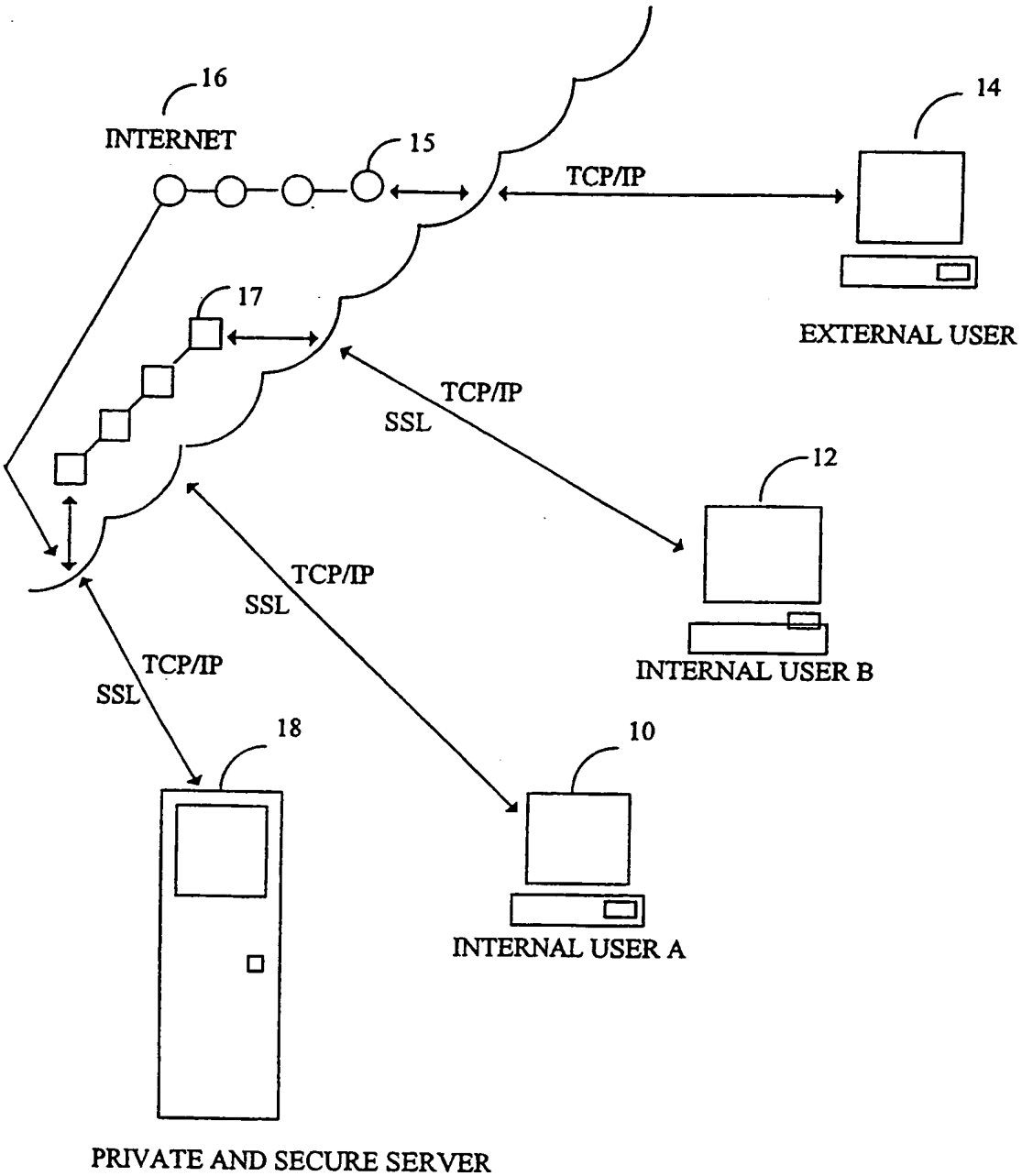


Figure 2 OSI Interface for standard network architecture

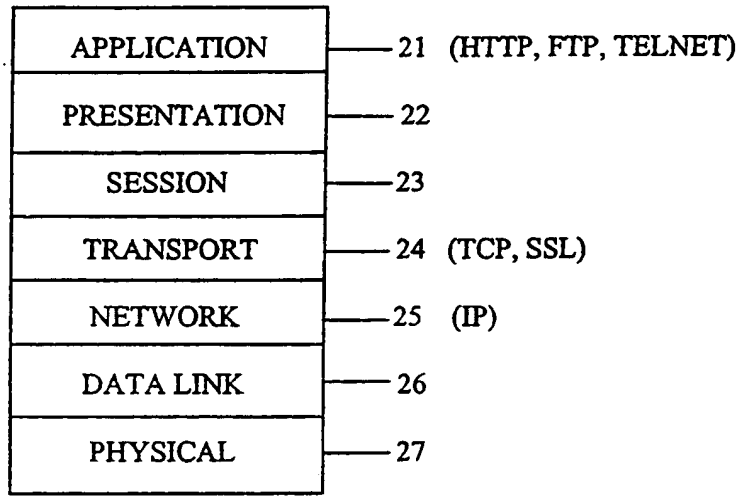


Figure 3 Sending a secure document via SSL

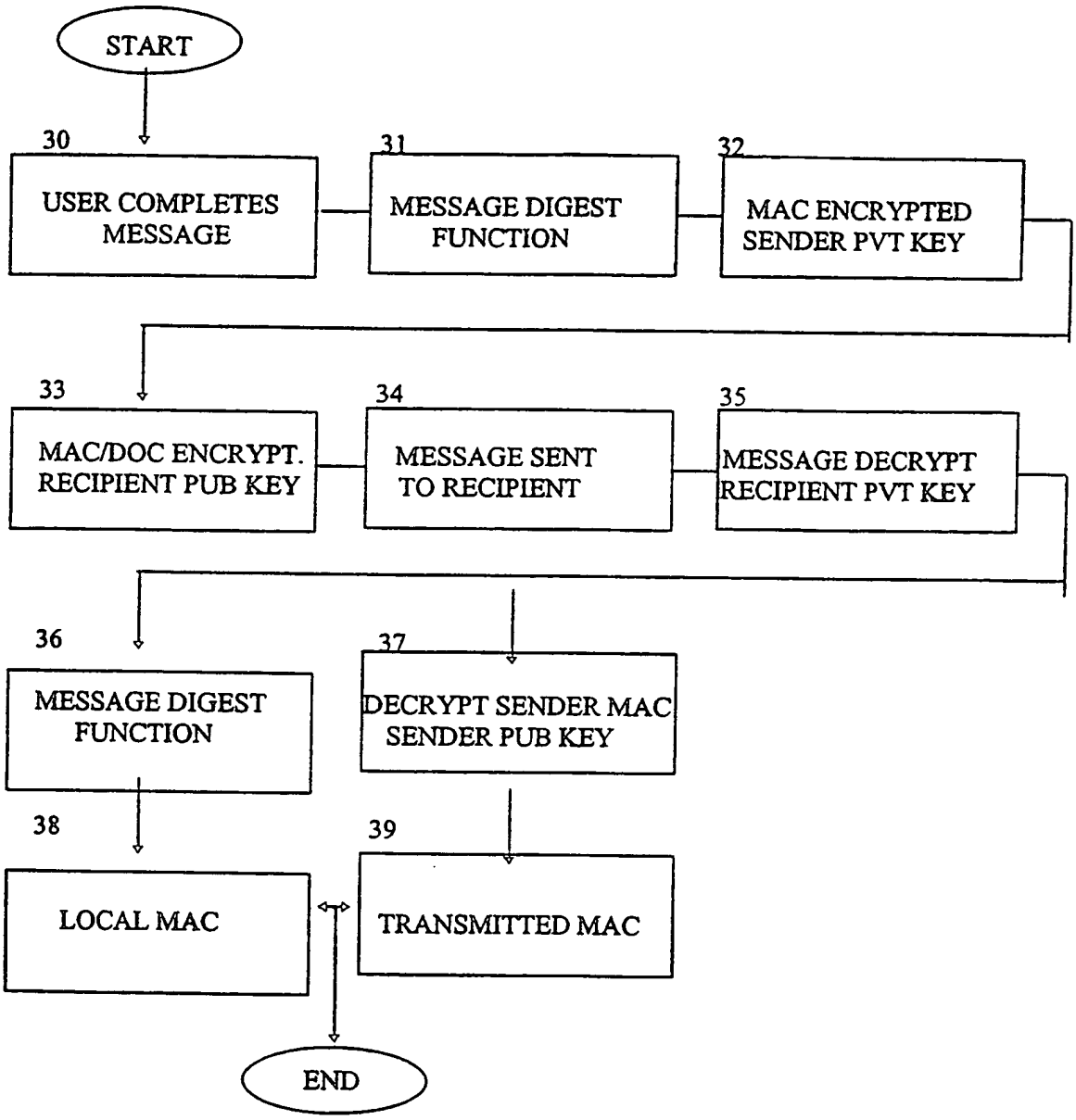


Figure 4 Internal User sends message to Internal or External User

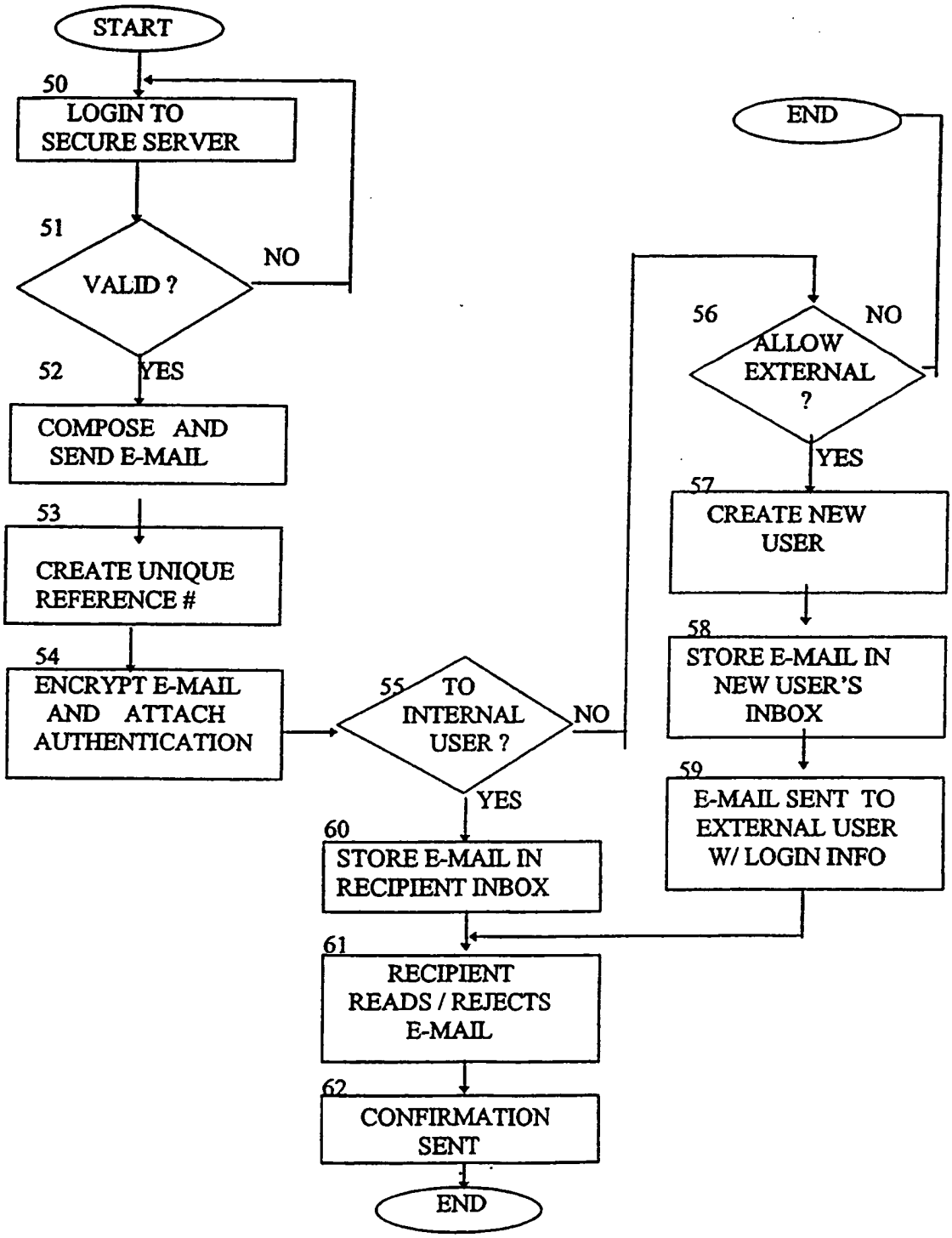


Figure 5 External User sends message to Internal User

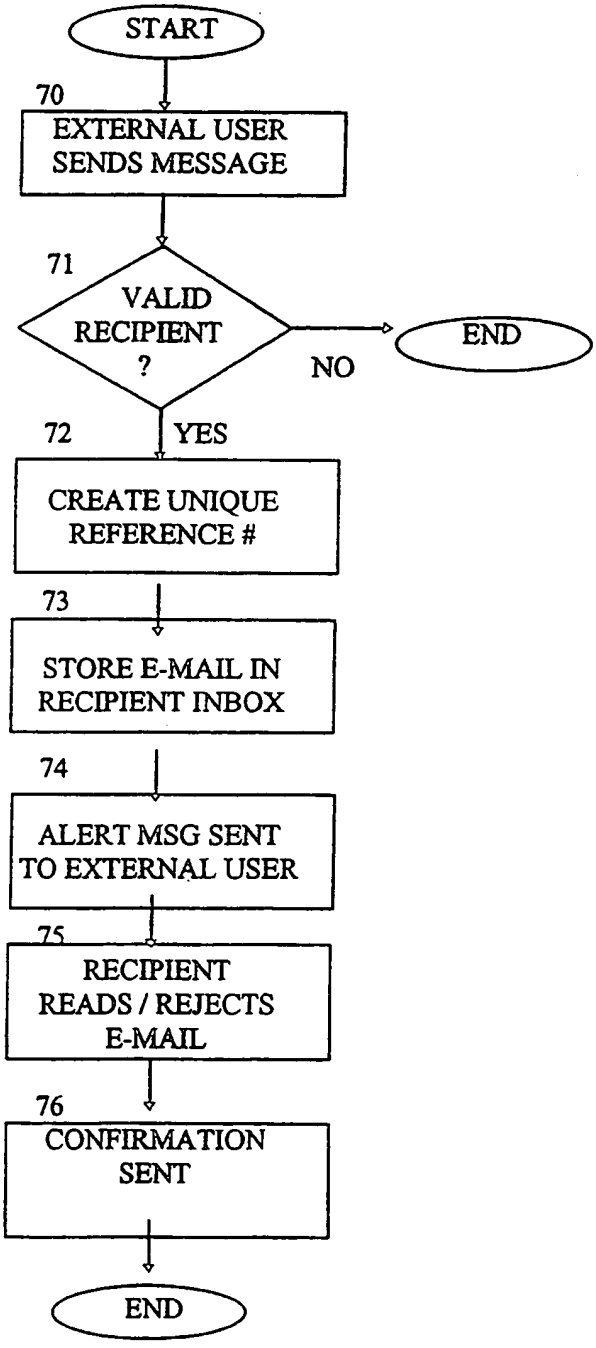


Figure 6

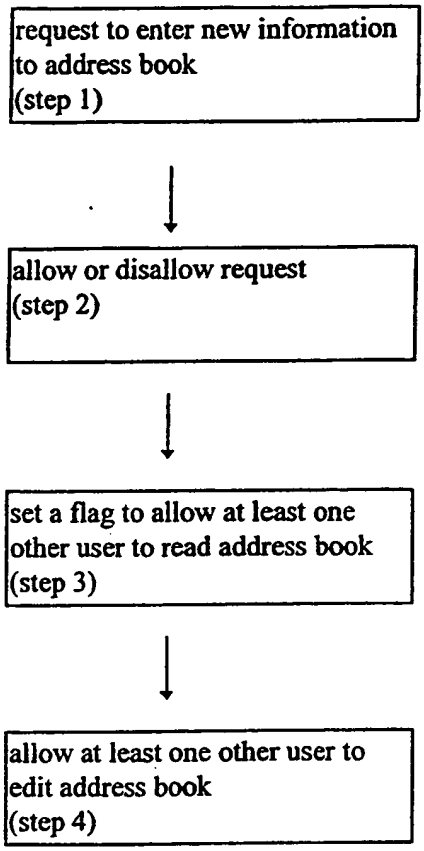

request to enter new information to address book (step 1)
allow or disallow request (step 2)
set a flag to allow at least one other user to read address book (step 3)
allow at least one other user to edit address book (step 4)

Figure 7

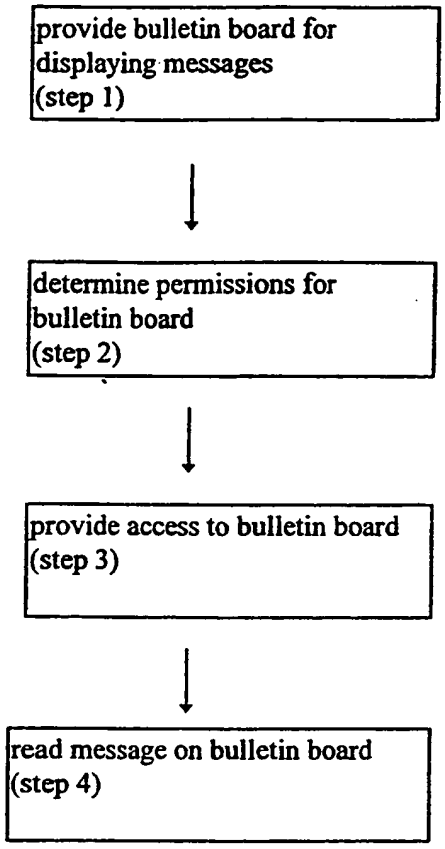
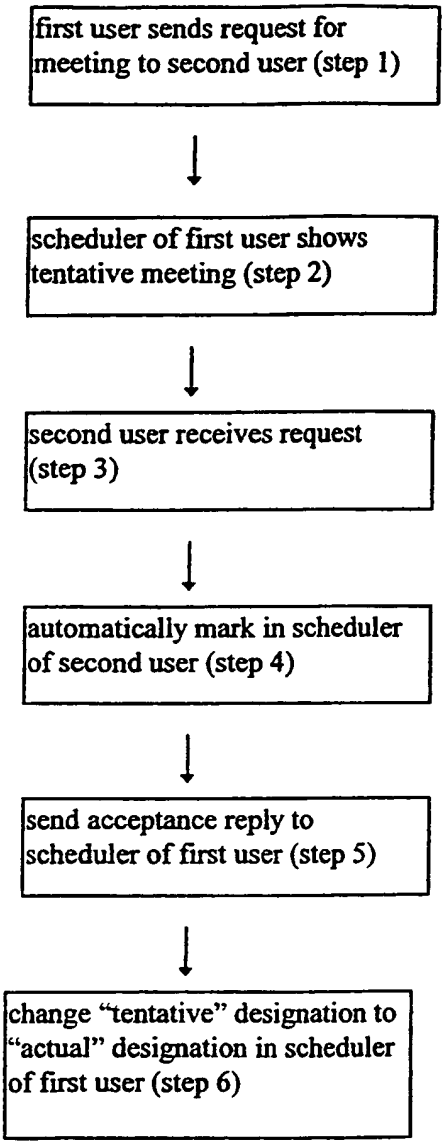

provide bulletin board for displaying messages (step 1)
determine permissions for bulletin board (step 2)
provide access to bulletin board (step 3)
read message on bulletin board (step 4)

Figure 8



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL99/00549

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :713/150, 151

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/150, 151

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,790,790 A (SMITH et al) 04 AUGUST 1998, abstract, col 2 lines 20-31, col 3 lines 22-25 and 47-62, col 4 lines 1-14, col 5 lines 17-36, col 6 lines 64-67, col 7 lines 1-10 and 28-48, col 8 lines 7-8 and 29-51 col 10 lines 48-67, col 11 lines 1-4	1-15, 18-24, 26-39 ---- 16, 17, 25
Y	SSL Protocol Version 3.0 Internet Draft, sections 5.6.2, 5.6.6, and D.3., 18 nOVEMBER 1996.	16, 17, 25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

°	Special categories of cited documents:	°T°	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
°A°	document defining the general state of the art which is not considered to be of particular relevance	°X°	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
°E°	earlier document published on or after the international filing date	°Y°	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
°L°	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	°&°	document member of the same patent family
°O°	document referring to an oral disclosure, use, exhibition or other means		
°P°	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 17 FEBRUARY 2000	Date of mailing of the international search report 21 MAR 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 308-3900

Form PCT/ISA/210 (second sheet)(July 1992)☆